Validación de identidades mediante las mallas de confianza OpenPGP

En búsqueda de la sostenibilidad

Gunnar Eyal Wolf Iszaevich • Jorge Luis Ortega Arjona

6° Foro de Seguridad de la Información • CICESE • 2021.09.30

Había una vez una red ingenua y feliz. . .

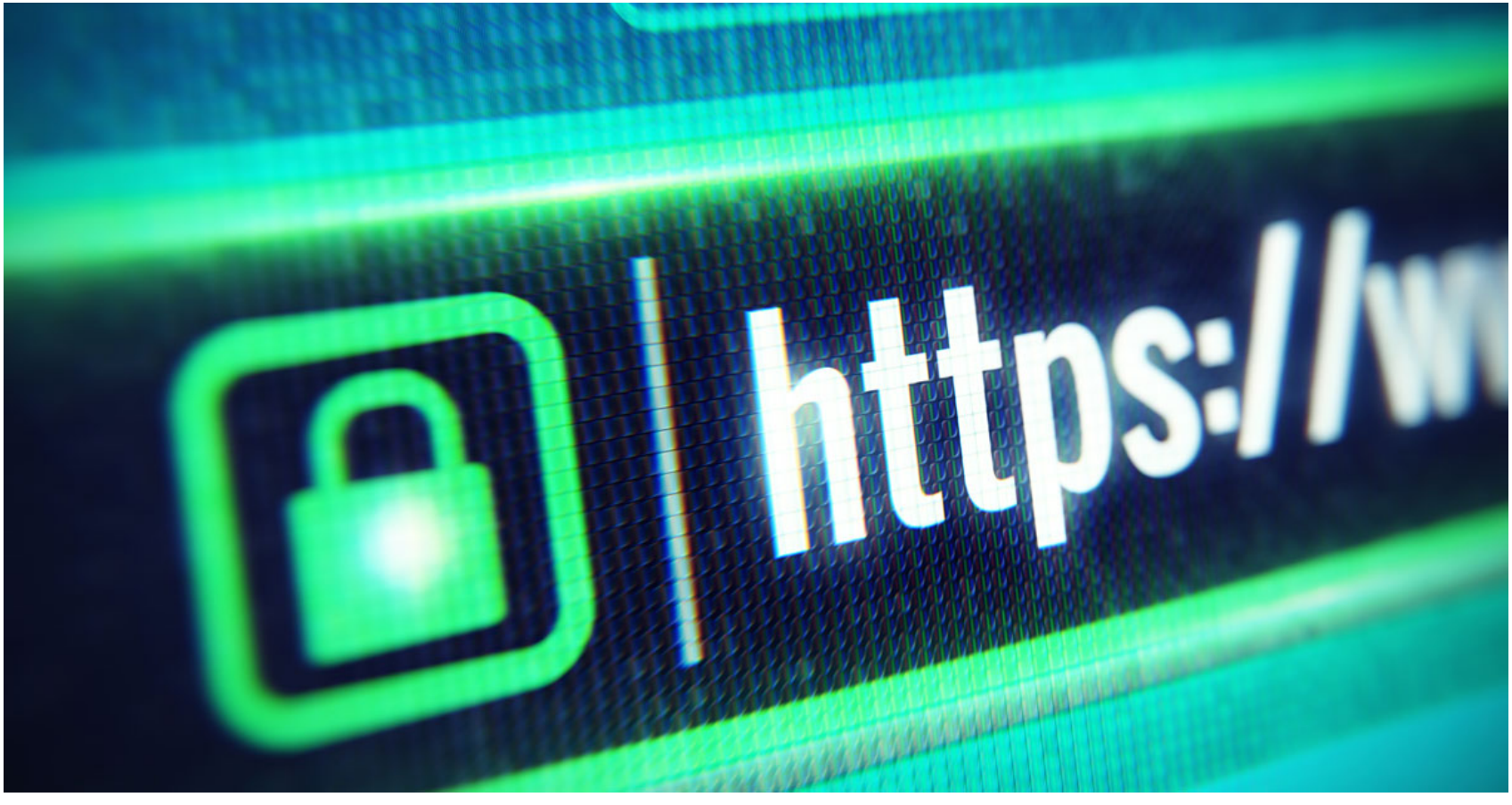
freepngimg.com (Atribución)

Happy Computer, archive.org (CC BY-NC-ND)

Pero el mundo es malo, malo

positek.net / shutterstock (CC BY-SA)

Afortunadamente Internet ha evolucionado: ¡El cifrado está en todas partes!



Pero... ¿Qué es lo que este cifrado realmente nos brinda?

Protección contra escuchas indeseables

Alex Briseño, Flickr (CC BY-SA-NC)

¿Que nos brinda el simple *cifrado de llave pública*? ¿Y qué sigue sin cubrir?

Obtenemos

- Criptografía fuerte
  - Imposible de romper con los recursos de un Estado-Nación contemporáneo
- Uso de algoritmos que han tenido escrutinio público
  - ElGamal, DSA, RSA
- Empleo sobre protocolos preexistentes
  - Almacenamiento local, correo electrónico

No nos brinda

- Ocultamiento del *hecho de que hay comunicación* entre dos participantes
  - Análisis de metadatos
- Comprobación de identidad correcta
  - Ataques de suplantación
  - Ataques de *Hombre en el Medio* (MITM)

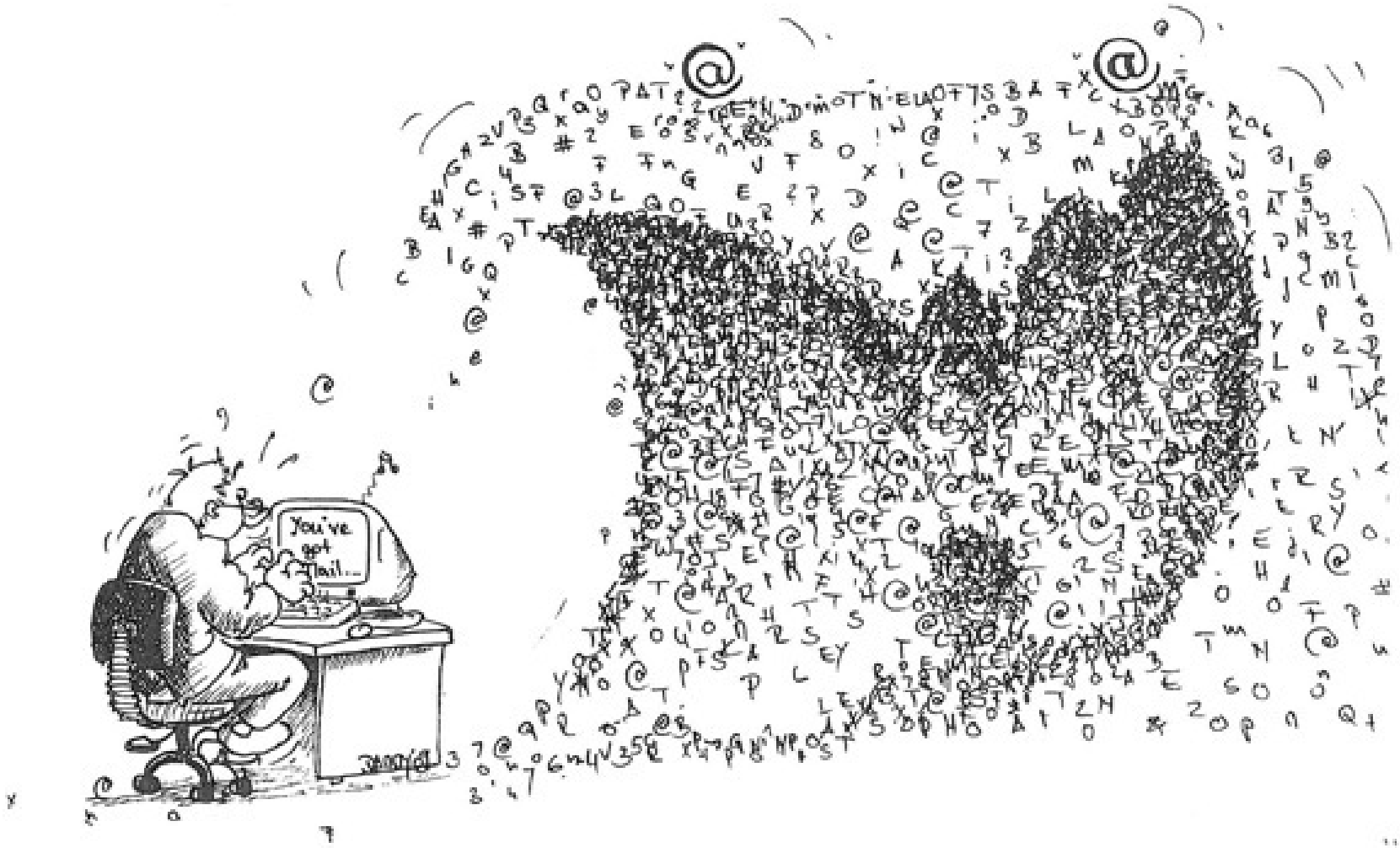
PGP: Pretty Good Privacy

30 años volando alto

Bloques de construcción para la *verificación de identidad*

Pero... ¿Cómo *verificamos* la identidad?

Internet es demasiado grande como para *conocerlos* a todos. . .

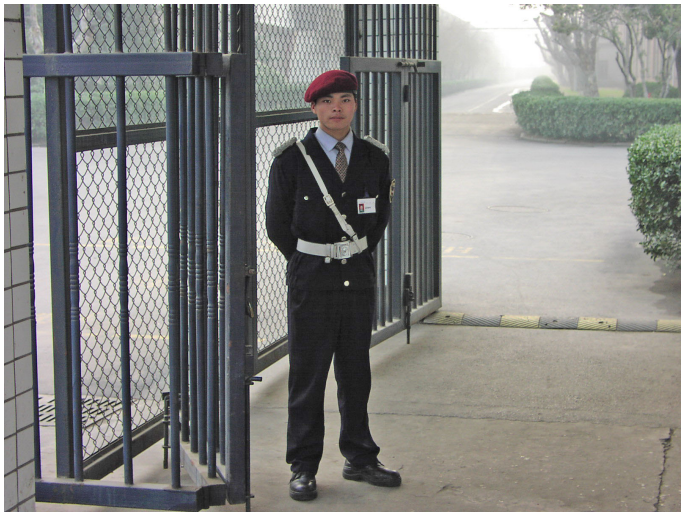


Mecanismos transitivos de distribución de confianza

. . . Pero en *alguien* podremos confiar, ¿cierto?

Y podemos confiar en la *veracidad* de las identidades que éste respalde.

1 Confianza centralizada



Robbie Sproule, Wikipedia (CC BY)
Francis Sarahi Castro Ponce, Wikipedia (CC 0)

everystockphoto.com, Wikipedia (DP)

2 Confianza distribuida

Miren Pardo, Juegos de asamblea: Conocemos a nuestros compañeros (CC BY-SA-NC)

Formalicemos un poquito, por favor...

Mecanismos centralizados

- Se definen (centralmente) algunas *raíces de confianza*
- Las *raíces de confianza* pueden delegar confianza a varias *autoridades certificadoras* (CA)
- Cada servidor proporciona su llave criptográfica y un *certificado*, firmado por una CA

$\Downarrow$

Modelo PKI-CA

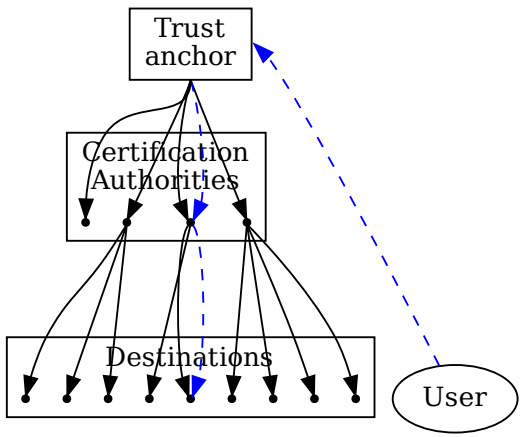
Mecanismos distribuidos

- Centrados en *cada usuario*
- Cada usuario puede *emitir certificados* para quien conozca personalmente
  - ¿Políticas de firmado?
  - ¿Qué es conocer?
- Se crea una *malla de confianza* (*Web of Trust*) global

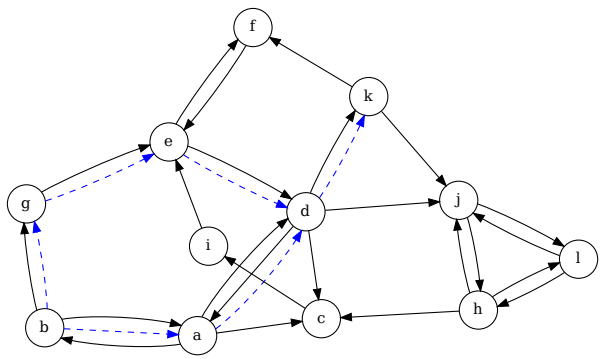
$\Downarrow$

Modelo WoT

Modelos de distribución de confianza



Centralizado: Autoridades Certificadoras (PKI-CA)



Distribuido: Malla de Confianza (WoT)

Enfoque del trabajo: Modelo distribuido (WoT)

. . . Pero eso depende de que *muchos* se conozcan con *muchos*

Steven Fruitsmaak, WikiNews (CC BY)

Entonces, ¿lo único que hace falta es *crecer* las redes de firmado?

- Todos verificamos nuestros mutuos doumentos
- *Certificamos* las llaves del resto del grupo
- ¡Aumentamos la confiabilidad de la red!

Steven Fruitsmaak, WikiNews (CC BY)

Entonces, ¿lo único que hace falta es *crecer* las redes de firmado?

- Todos verificamos nuestros mutuos doumentos
- *Certificamos* las llaves del resto del grupo
- ¡Aumentamos la confiabilidad de la red!

- . . . En *eventos* de hasta 300 personas. ¿En serio?

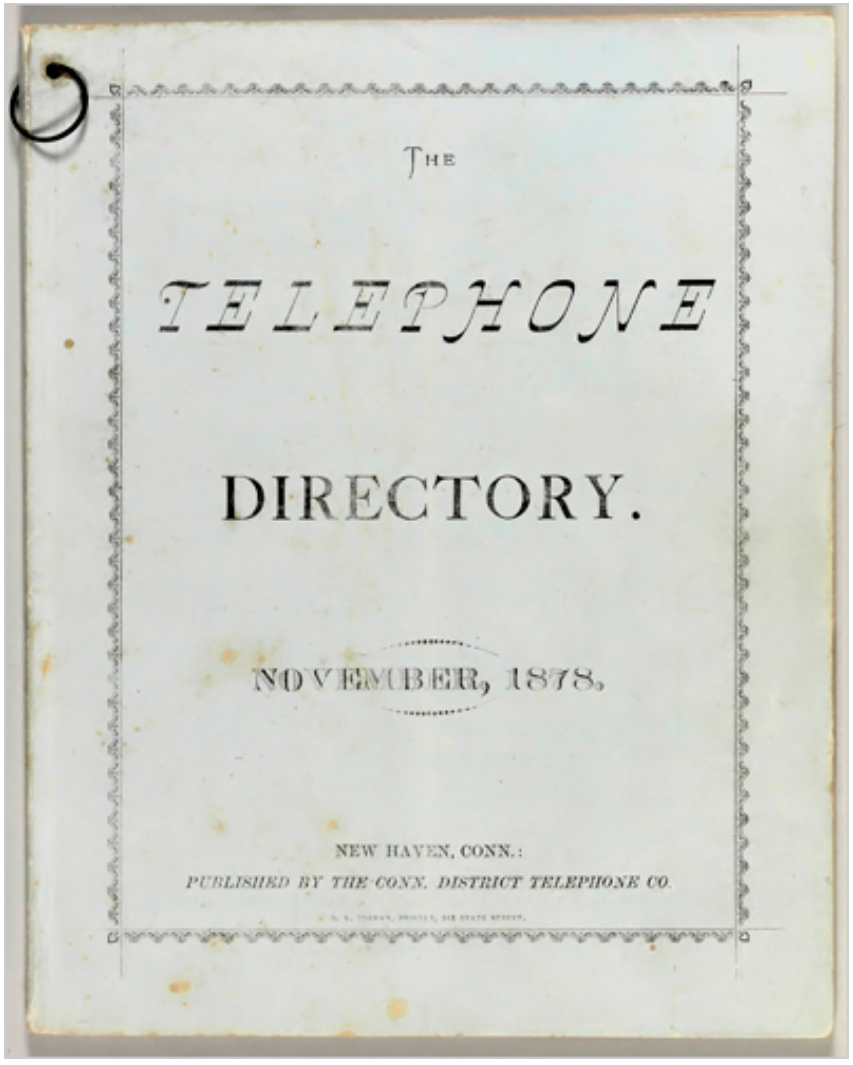
Steven Fruitsmaak, WikiNews (CC BY)

El problema de la distribución *de las llaves públicas*

Es necesaria una *infraestructura de distribución* de llaves

- Bajo PKI-CA (TLS), llave+firmas se entregan al establecerse una sesión
  - ¡Ojo con MitM, revocaciones!
- Bajo WoT (OpenPGP), la llave debe obtenerse *antes de* preparar un mensaje
  - Operación asíncrona

$\Rightarrow$ Red de servidores HKP


THE

TELEPHONE

DIRECTORY.

NOVEMBER, 1878.

NEW HAVEN, CONN.:

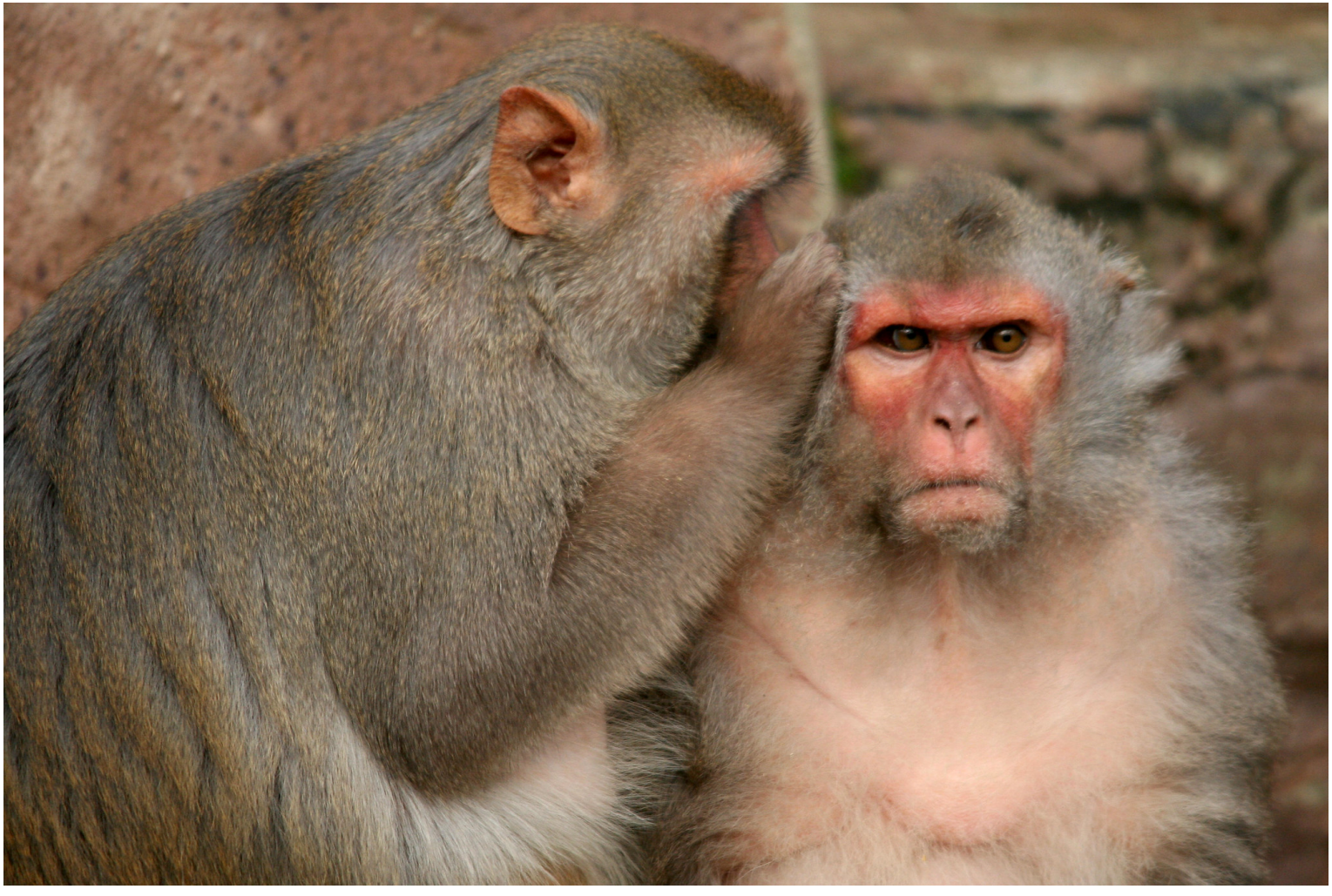
PUBLISHED BY THE CONN. DISTRICT TELEPHONE CO.

Connecticut District Telephone Company, 1878 (DP)

Pero... ¿y lo de evitar la centralización?

Javier Álvarez, Flickr (CC BY-ND)

Protocolo *de chisme* o *epidémico* para reconciliación de conjuntos grandes



jinterwas, Flickr (CC BY)

Resultado (1): Almacenamiento binario, no-modificable, distribuido, no-autenticado, eventualmente consistente

Resultado ②: ataques al modelo ☹

Ben Simon (CC BY)

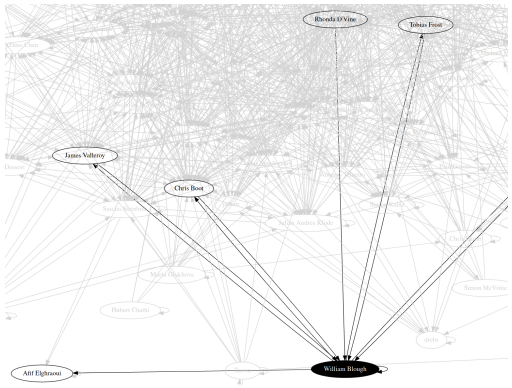
)

jinterwas, Flickr (CC BY)

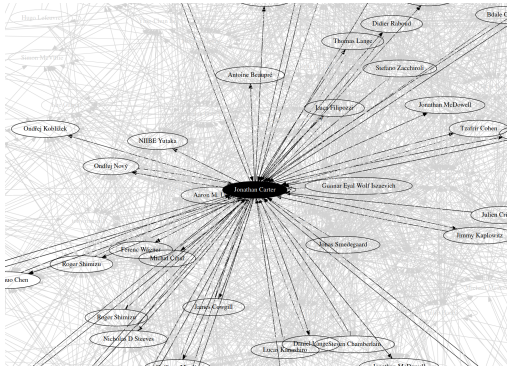
¿Qué es el *envenenamiento de certificados*? (1)

Normalmente, mis conocidos directos *certifican* mi llave, permitiendo a cualquiera encontrarme en la WoT

Puedo estar poco conectado...



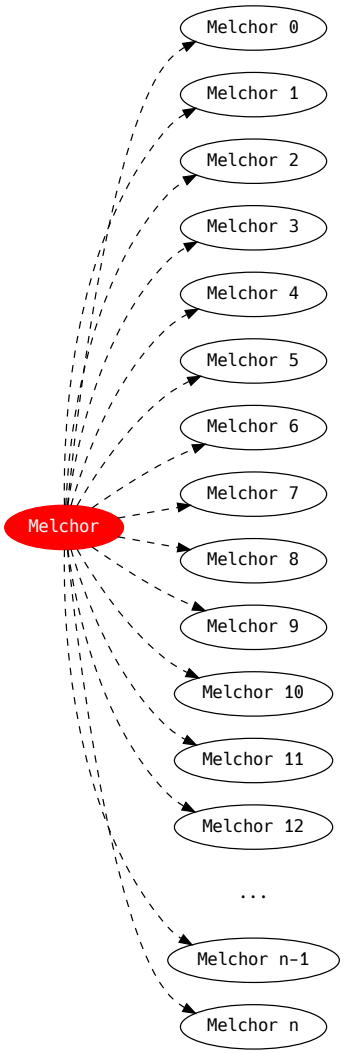
Puedo estar medianamente conectado...



Puedo estar *muy* conectado...

Del orden de decenas, tal vez hasta *cientos* de certificados por llave en circunstancias normales

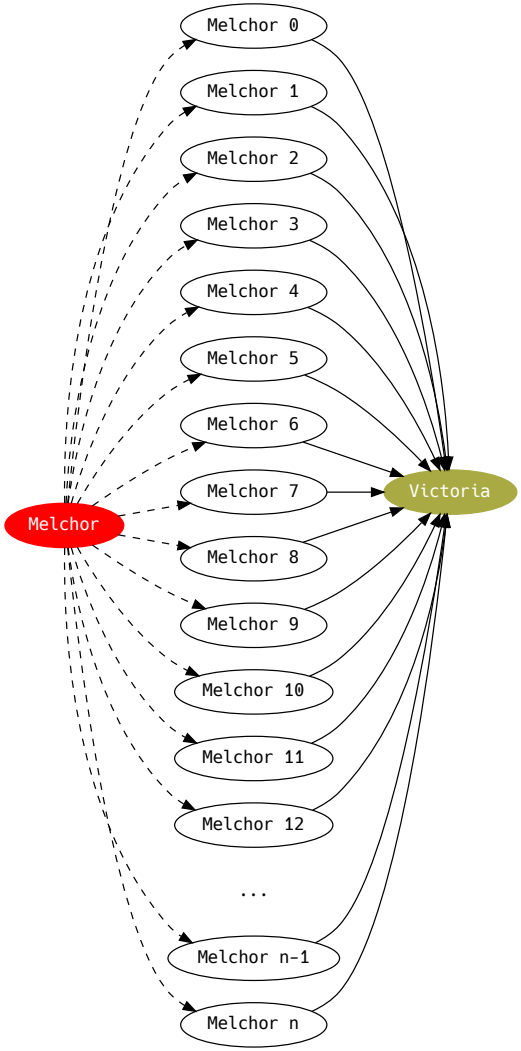
¿Qué es el *envenenamiento de certificados*? (2)



Un atacante *Melchor* (M) genera *muchas* identidades descartables $M_1, M_2, M_3, ...M_n$ ($n \approx 100\,000$)

Estas identidades son *llaves basura*, no necesitan ser de ninguna manera *relacionables* con la identidad de *Melchor*.

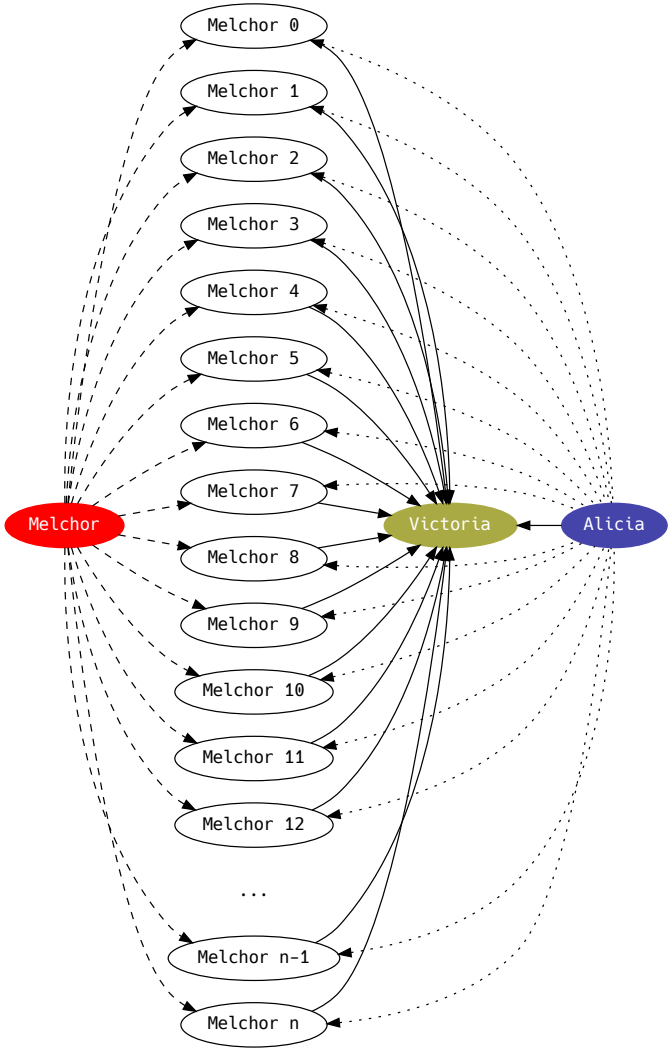
¿Qué es el *envenenamiento de certificados*? (3)



Certificar la llave de su víctima, *Victoria* (V), con todas estas identidades — e inutilizar la llave pública V

Victoria puede verse obligada a abandonar su identidad y generar un nuevo par de llaves V', pero volver a vincularse a la WoT tiene un alto costo (tiempo, esfuerzo, ventana de oportunidad para suplantación)

¿Qué es el *envenenamiento de certificados*? (4)



Cuando *Alicia* (*A*) busca la llave de *Victoria*, al intentar importarla, sufre una negación de servicio (y posible corrupción de base de datos OpenPGP)

¿Qué es el *envenenamiento de certificados*? (5)

Peter Krimbacher, Wikipedia (CC BY-SA)

¿Y por qué no eliminar los certificados espurios?

Jumanji Solar, Flickr (CC BY-NC-SA)

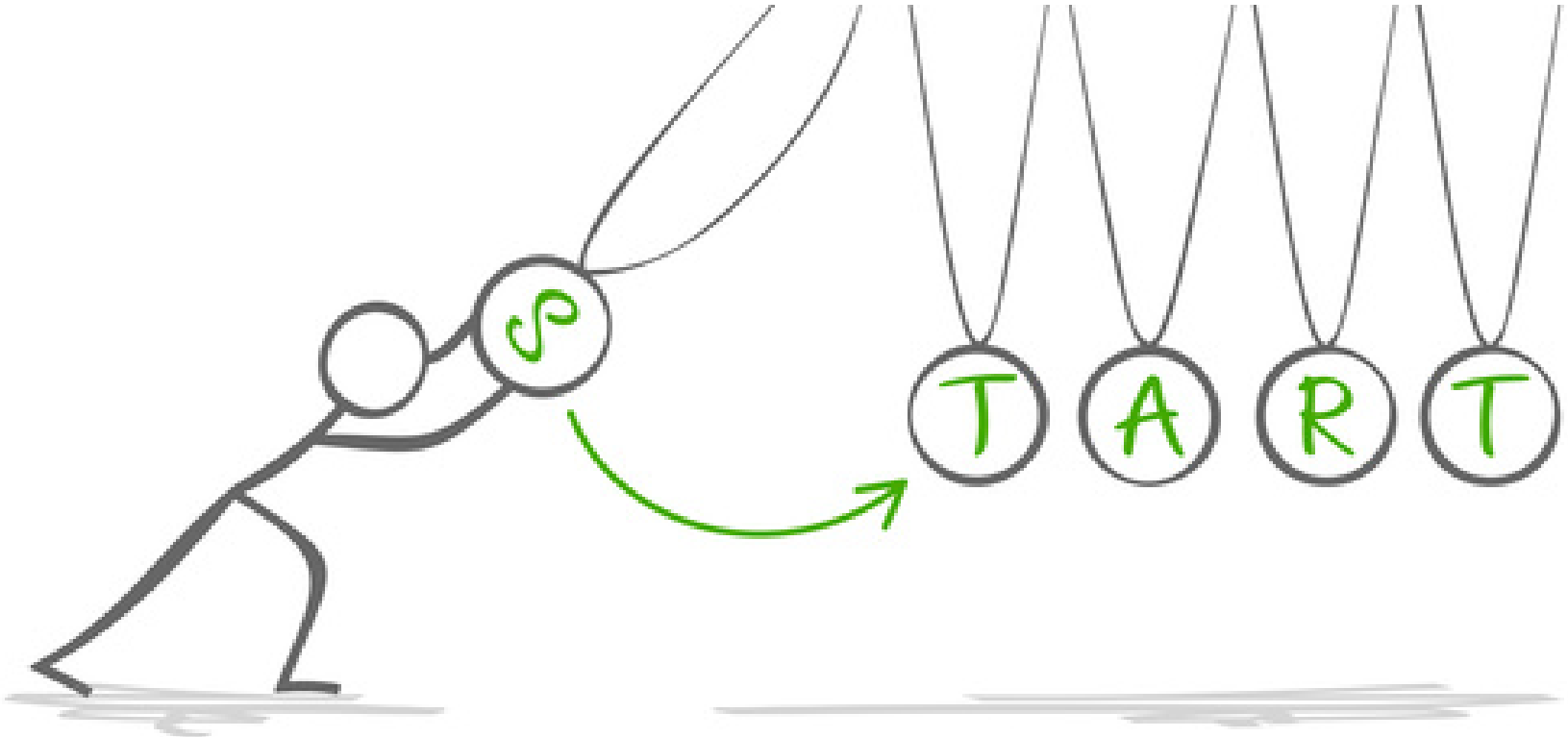
José-Manuel Benito, Wikimedia (DP)

¿Y por qué no eliminar los certificados espurios?

Jumanji Solar, Flickr (CC BY-NC-SA)

José-Manuel Benito, Wikimedia (DP)

Estado del proyecto



Otras implementaciones e ideas relacionadas

Sequoia-PGP

Hagrid Keyserver

Hockeypuck Keyserver

Varias otras. . . en *estado académico*

Mark Boulton (CC BY-SA)

)

European Southern Observatory, Flickr (CC-BY)

Idea central

Plantear una solución que mantenga la viabilidad del modelo distribuido, sin requerir de entidades centralizadoras.

Busco proponer un protocolo que contrarreste los principales ataques observados, principalmente al *envenenamiento de certificados*, sin comprometer las principales propiedades del modelo WoT.

Si se requere que todo paquete adicionado a k sea aceptado (firmado) por k, el envenenamiento de certificados deja de ser posible. Esto, además, llevaría la recomendación de comunicar nuevas firmas al destinatario y no directamente a la red de serivdores de una *buena práctica* al modelo base de operación.

Objetivos del proyecto

La implementación de este cambio en apariencia simple conlleva los siguientes objetivos:

- Permite que la red de servidores de llaves públicas descentralizada de OpenPGP continúe operando, mitigando el efecto que han tenido en ella ataques como el descrito
- El modelo descentralizado de confianza transitiva WoT puede mantenerse relevante y sostenible para las comunicaciones OpenPGP

Gracias por su atención